



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/566,504	01/31/2006	Karine Villegas	1032326-000330	7562
21839 7590 07/31/2007 BUCHANAN, INGERSOLL & ROONEY PC POST OFFICE BOX 1404 ALEXANDRIA, VA 22313-1404			EXAMINER PATEL, NIRAV B	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 07/31/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/566,504	<b>Applicant(s)</b> VILLEGAS ET AL.	
	<b>Examiner</b> Nirav Patel	<b>Art Unit</b> 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 1 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 15 May 2007.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-31 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☐ Claim(s) \_\_\_\_\_ is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☒ Claim(s) 1-31 are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. This action is responsive to the communication filed on May 15, 2007. Applicant's amendment filed on May 15, 2007 has been entered. Claims 1-31 are pending. The Office would like to notify the Applicant that there has been a change in the Examiner to conduct the future examination and prosecution process of the currently pending application.

### Election/Restrictions

2. This application contains claims directed to the following patentably distinct species:
  - a. Species 1: associates with Claims 1-14, 29, 30.
  - b. Species 2: associate with Claims 15-28, 31
3. The Species are independent or distinct because each of the various disclosed Species details specific characteristic of the following:
  - a) A method of securely implementing a public-key cryptography algorithm in a microprocessor-based system, the public key being composed of an integer  $n$  that is a product of two large prime numbers  $p$  and  $q$ , and of a public exponent  $e$ , **said algorithm also including a private key**, said method determining a set  $E$  comprising a predetermined number of prime

Art Unit: 2135

numbers  $e_i$  that can correspond to the value of the public exponent  $e$ , and comprising the following steps: a) **computing a value  $\Phi = \prod e_i$**

$$e_i \in E$$

such that  $\Phi/e_i$  is less than  $\Phi(n)$  for any  $e_i$  belonging to  $E$ , where  $\Phi$  is the Euler totient function; b) **applying the value  $\Phi$  to a predetermined computation involving, as a modular product, only the modular product of  $\Phi$  multiplied by said private key of the algorithm;** c) for each  $e_i$ , testing whether the result of said predetermined computation is equal to a value  $\Phi/e_i$ ...

- b. A method of securely implementing a public-key cryptography algorithm in a microprocessor-based system, the public key being composed of an integer  $n$  that is a product of two large prime numbers  $p$  and  $q$ , and of a public exponent  $e$ , said method determining a set  $E$  comprising a predetermined number of prime numbers  $e_i$  that can correspond to the value of the public exponent  $e$ , and comprising the following steps a) **choosing a value  $e_i$  from the values of the set  $E$ ;** b) **if  $\Phi(p) = \Phi(q)$ , where  $\Phi(n)$ ,  $\Phi(p)$ , and  $\Phi(q)$  are functions giving the number of bits encoding respectively the number  $n$ , the number  $p$ , and the number  $q$ ,** testing whether the **chosen  $e_i$  value satisfies the relationship:  $(1-e_i.d)$  modulo  $n < e_i \cdot 2^{(\Phi(n)/2)+1}$  or said relationship as simplified:  $(-e_i.d)$  modulo**

$n \leq e_i \cdot 2^{(\Phi(n)/2)+1}$  c) if the test relationship applied in the preceding step is satisfied, defining  $e = e_i \dots$

4. Applicant is required under 35 U.S.C. 121 to elect a single disclosed species for prosecution on the merits to which the claims shall be restricted if no generic claim is finally held to be allowable. Currently, no claims are generic.
5. Applicant is advised that a reply to this requirement must include an identification of the species that is elected consonant with this requirement, and a listing of all claims readable thereon, including any claims subsequently added. An argument that a claim is allowable or that all claims are generic is considered nonresponsive unless accompanied by an election.
6. Upon the allowance of a generic claim, applicant will be entitled to consideration of claims to additional species which depend from or otherwise require all the limitations of an allowable generic claim as provided by 37 CFR 1.411. If claims are added after the election, applicant must indicate which are readable upon the elected species. MPEP § 809.02 (a).
7. Applicant is advised that the reply to this requirement to be complete must include (i) an election of a species or invention to be examined even though the requirement be traversed (37 CFR 1.143) and (ii) identification of the claims encompassing the elected invention.
8. The election of an invention or species may be made with or without traverse. To reserve a right to petition, the election must be made with traverse. If the reply

does not distinctly and specifically point out supposed errors in the restriction requirement, the election shall be treated as an election without traverse.

9. Should applicant traverse on the ground that the inventions or species are not patentably distinct, Applicant should submit evidence or identify such evidence now or record showing the inventions or species to be obvious variants or clearly admit on the record that this is the case. In either instance, if Examiner finds one of the inventions unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103(a) of the other invention.
10. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).
11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

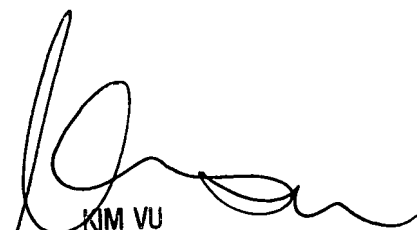
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

*NBP*

7/24/07



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100